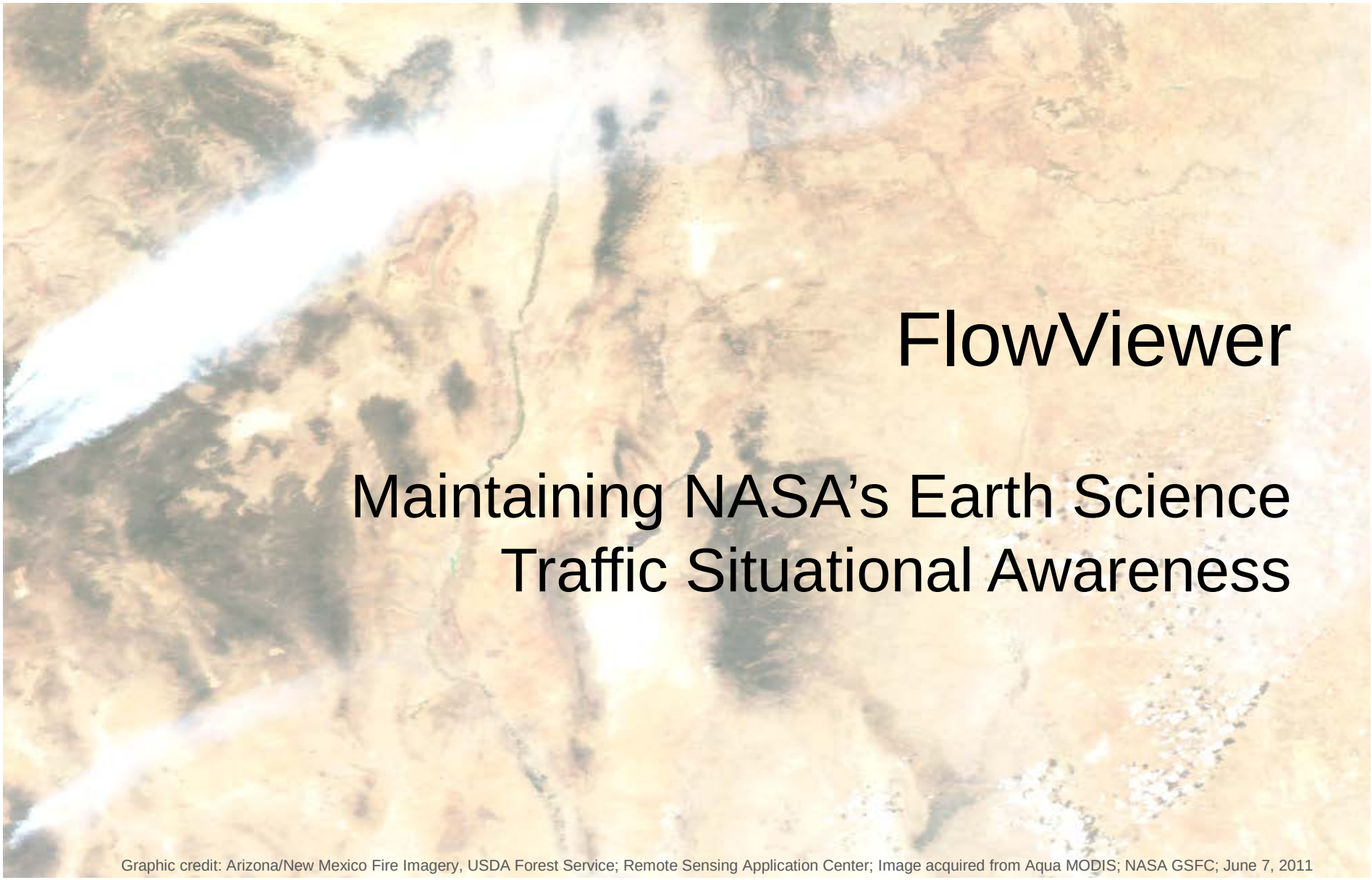


FlowViewer

Maintaining NASA's Earth Science Traffic Situational Awareness

Graphic credit: Arizona/New Mexico Fire Imagery, USDA Forest Service; Remote Sensing Application Center; Image acquired from Aqua MODIS; NASA GSFC; June 7, 2011

FlowViewer provides a convenient web-based user interface to Mark Fullmer's flow-tools suite, and now with v4.0, CMU NetSA group's SiLK. The inclusion of the underlying SiLK tool set enables FlowViewer users to continue to use the tool with the newer IPFIX netflow data protocol.

FlowViewer has been developed for NASA's Earth Sciences Data and Information System (ESDIS) networks, and credit goes to NASA for their usual outstanding support of innovation.

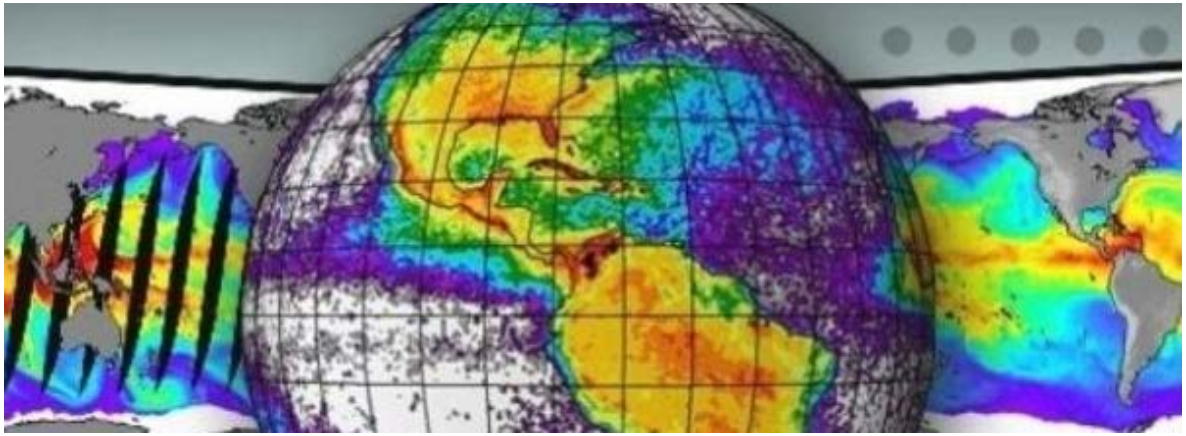
Graphic credit; Hurricane Sandy, October 29, 2012 Captured by Aqua MODIS; EOSDIS Website; NASA official: Kevin Murphy

- Complete open-source netflow collector analyzer
- Web-based UI provides dynamic front-end to open source collectors
- Dashboard provides user keep network traffic 'situational awareness'
- Ability to analyze IPFIX netflow (e.g., v9) data captured by SiLK
- Ability to continue to support netflow v5 installations via flow-tools
- Users can graph filtered traffic sets across a specified time period
- Background software tracks filtered traffic over long-term (ala MRTG)
- Ability to save filters and reports for later use and review
- Users can be alerted by email to abnormal data traffic situations

NASA Earth Science Network use of Netflow Data

EOSDIS NASA's Earth Observing System Data and Information System

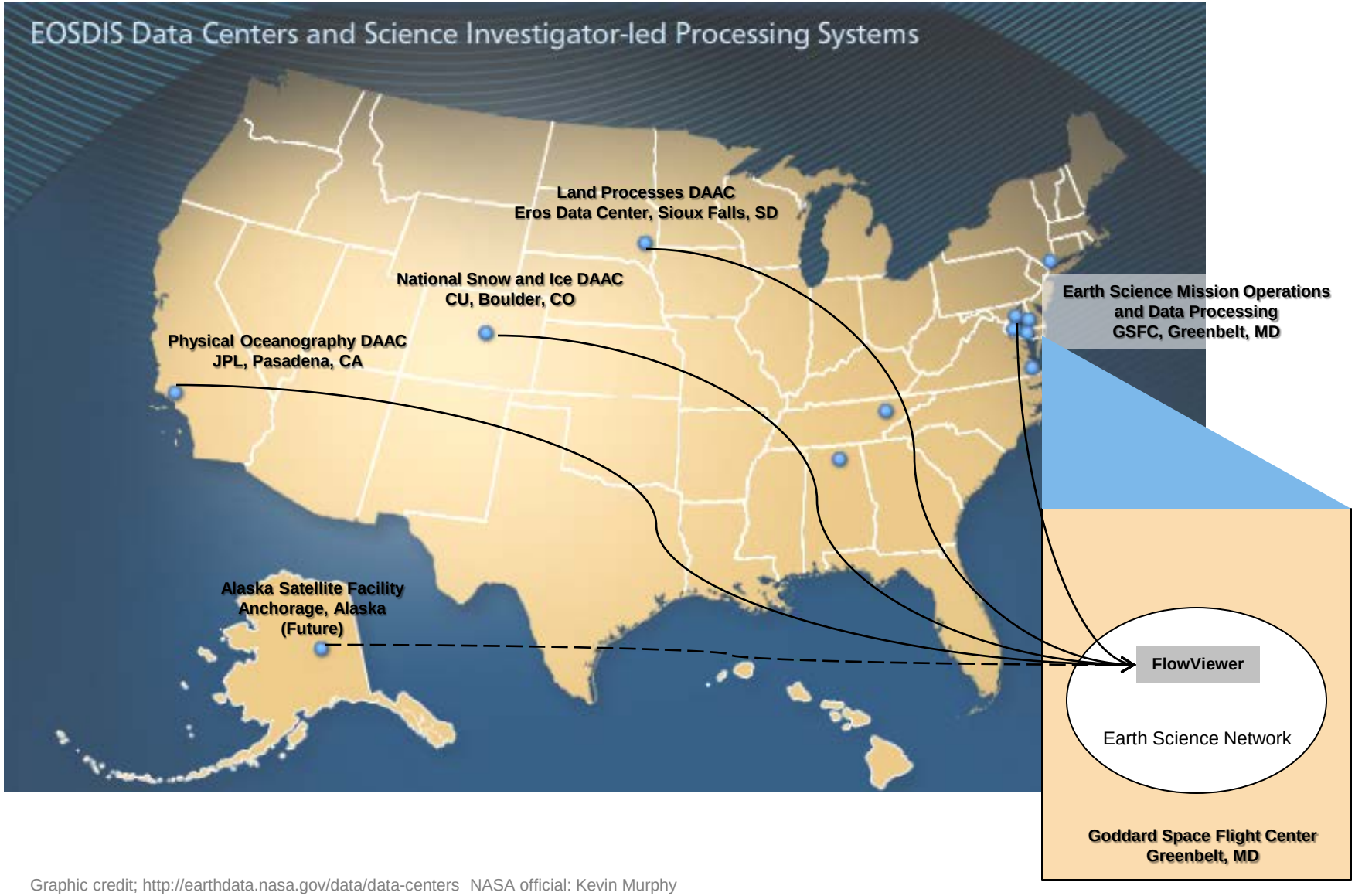
The Earth Observing System Data and Information System (EOSDIS) is a core capability in NASA's Earth Science Data Systems Program. It provides end-to-end capabilities for managing NASA's Earth science data from various sources – satellites, aircraft, field measurements, and various other programs. The EOSDIS serves a broad international community of Earth Science and meteorological scientists and users. Several TBytes of satellite and science data traverse its network every day.



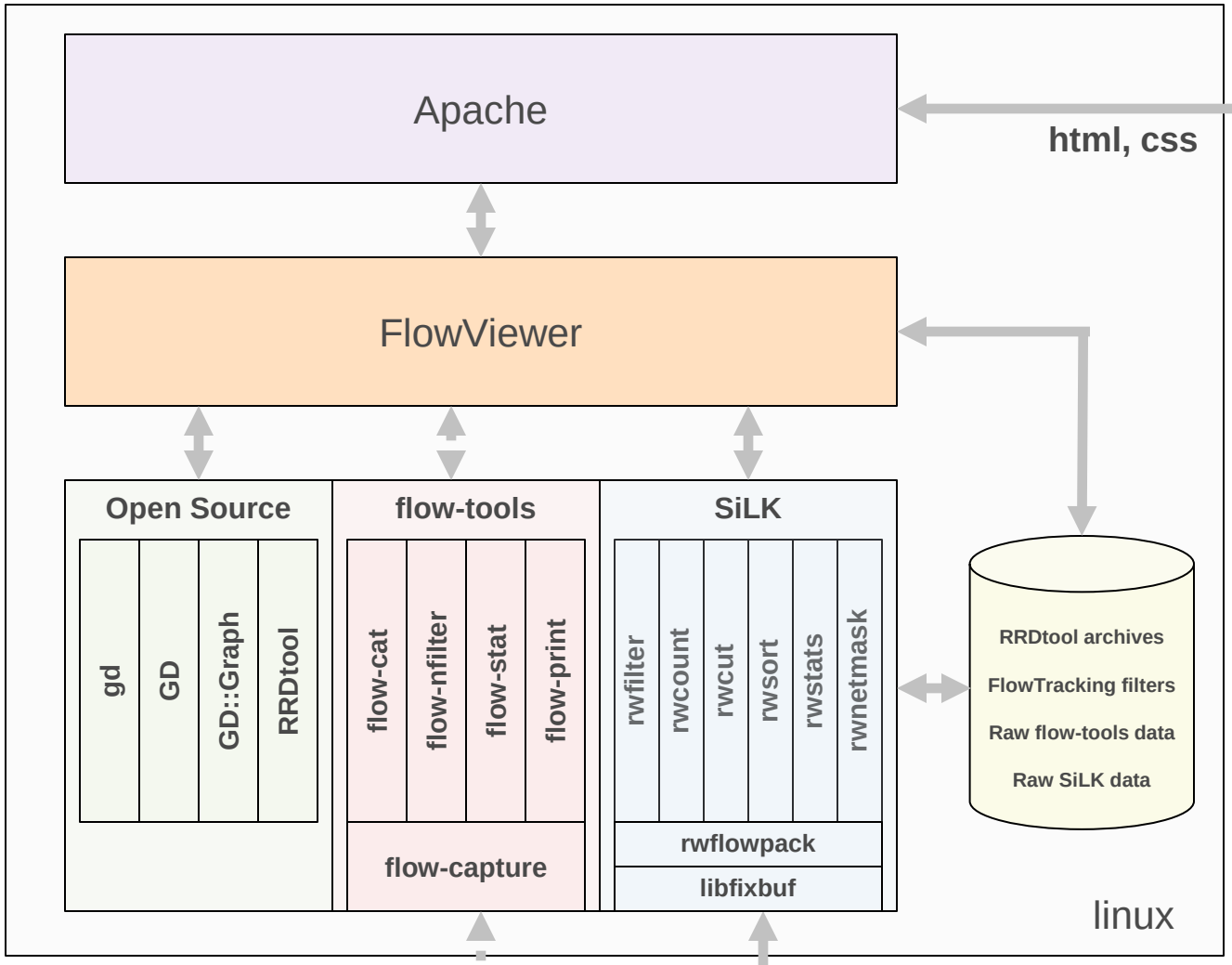
- In 2003 NASA and CSC worked to capture netflow data to help monitor traffic
- Initial capture/analysis system was based on *'cflowd'*
- FlowViewer was developed to aid traffic analysis (away from the command line)
- Today, NASA monitors over 200 Earth Science flows of interest (FlowTrackings)

Graphic credit; OPeNDAP is a data transport architecture and protocol widely used by Earth scientists to access remotely distributed data; EOSDIS Website; NASA official: Kevin Murphy

Netflow data sources

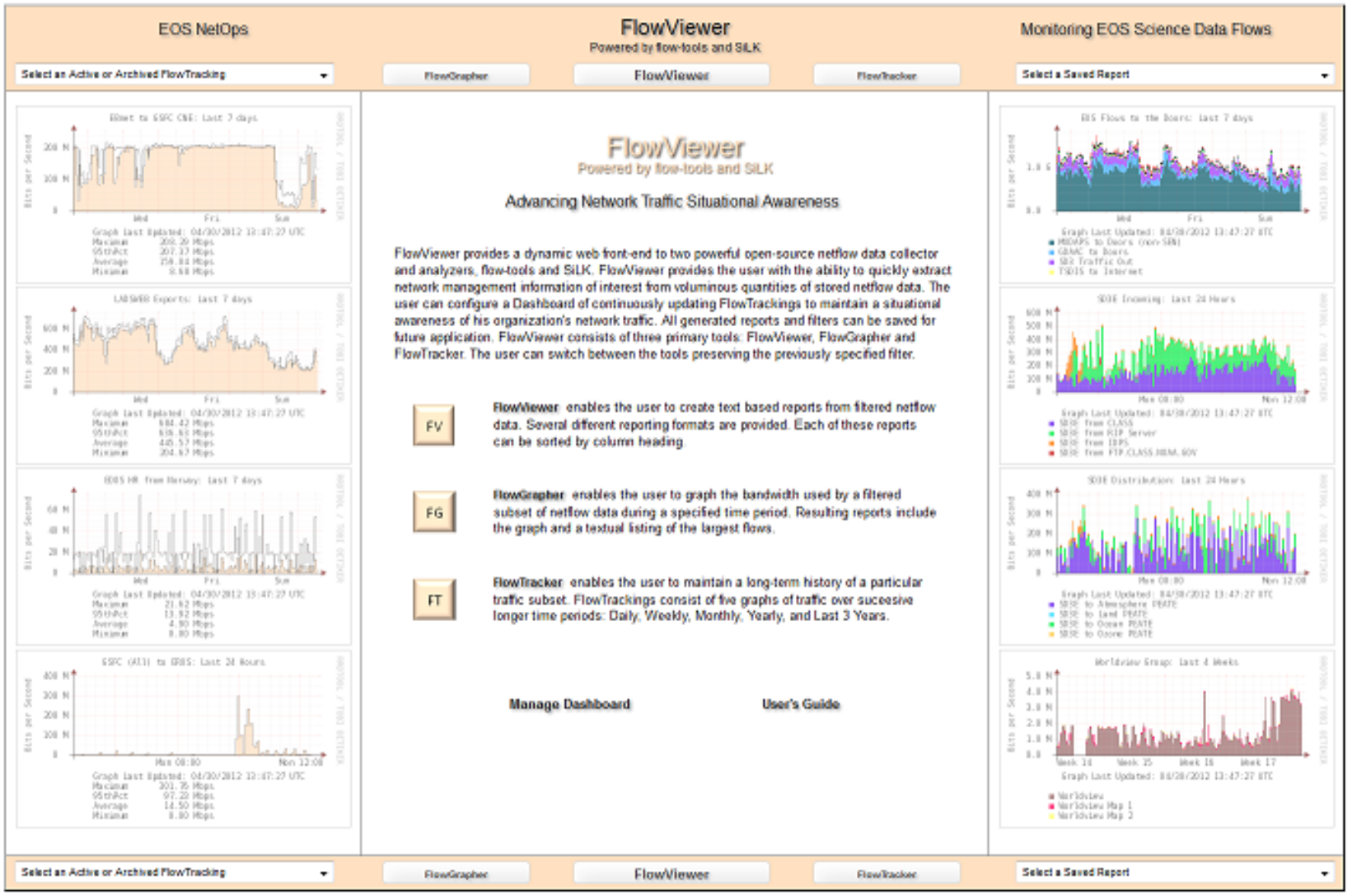


Graphic credit; http://earthdata.nasa.gov/data/data-centers NASA official: Kevin Murphy

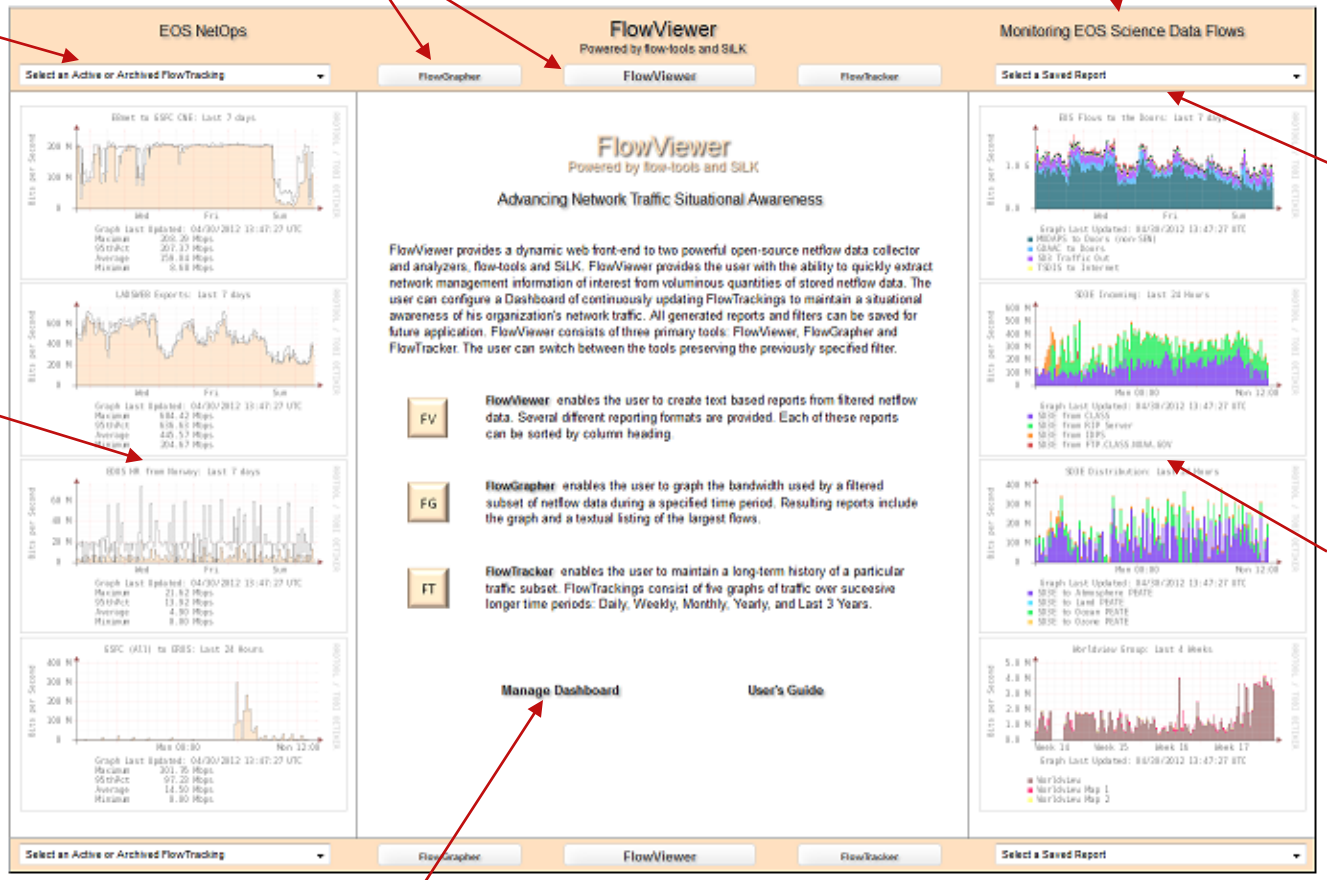


FlowViewer is an entirely open source netflow collector, analyzer and reporter. HTML/CSS user interface provides easy and wide deployability.

FlowViewer Main Screen

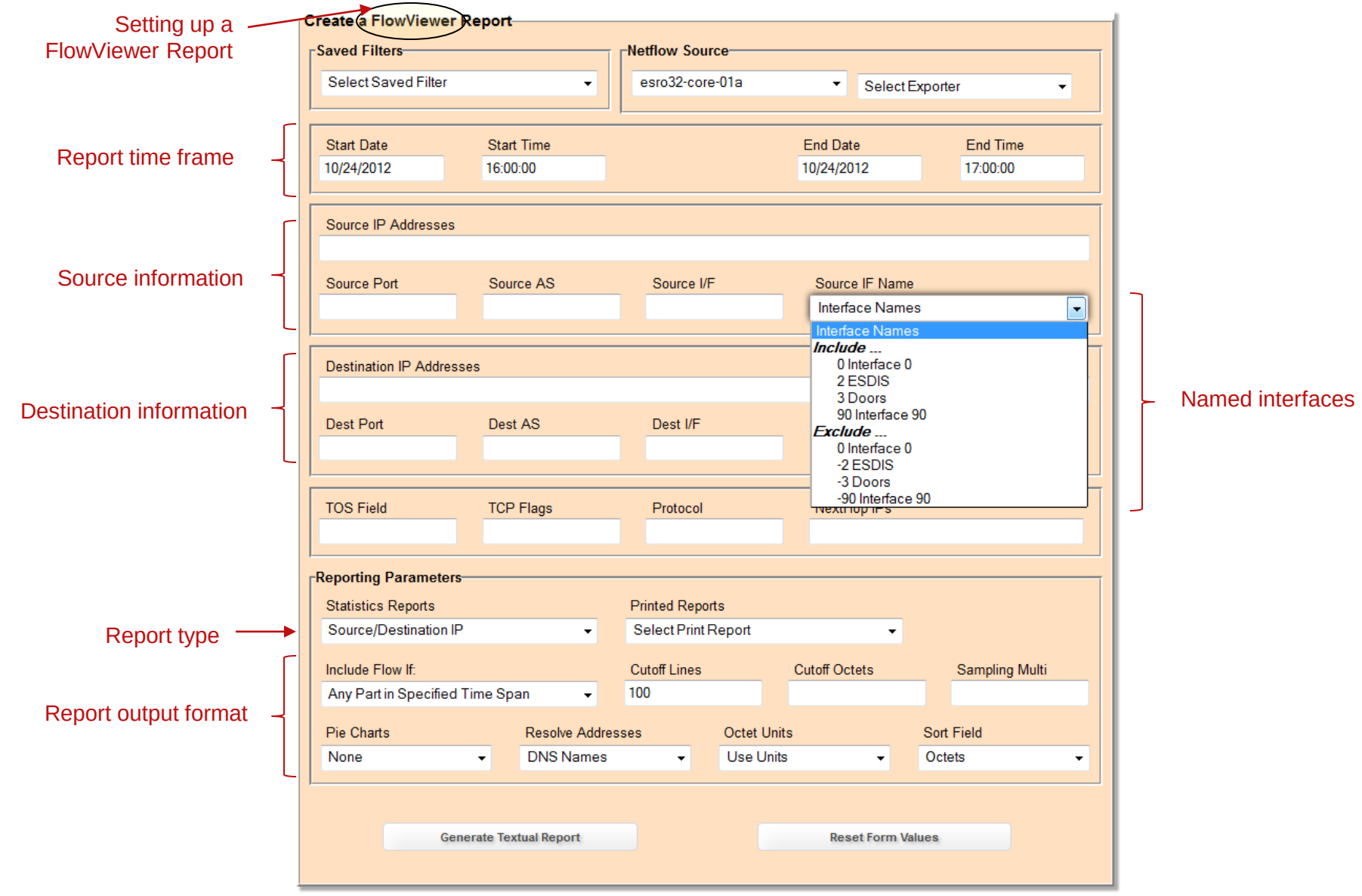


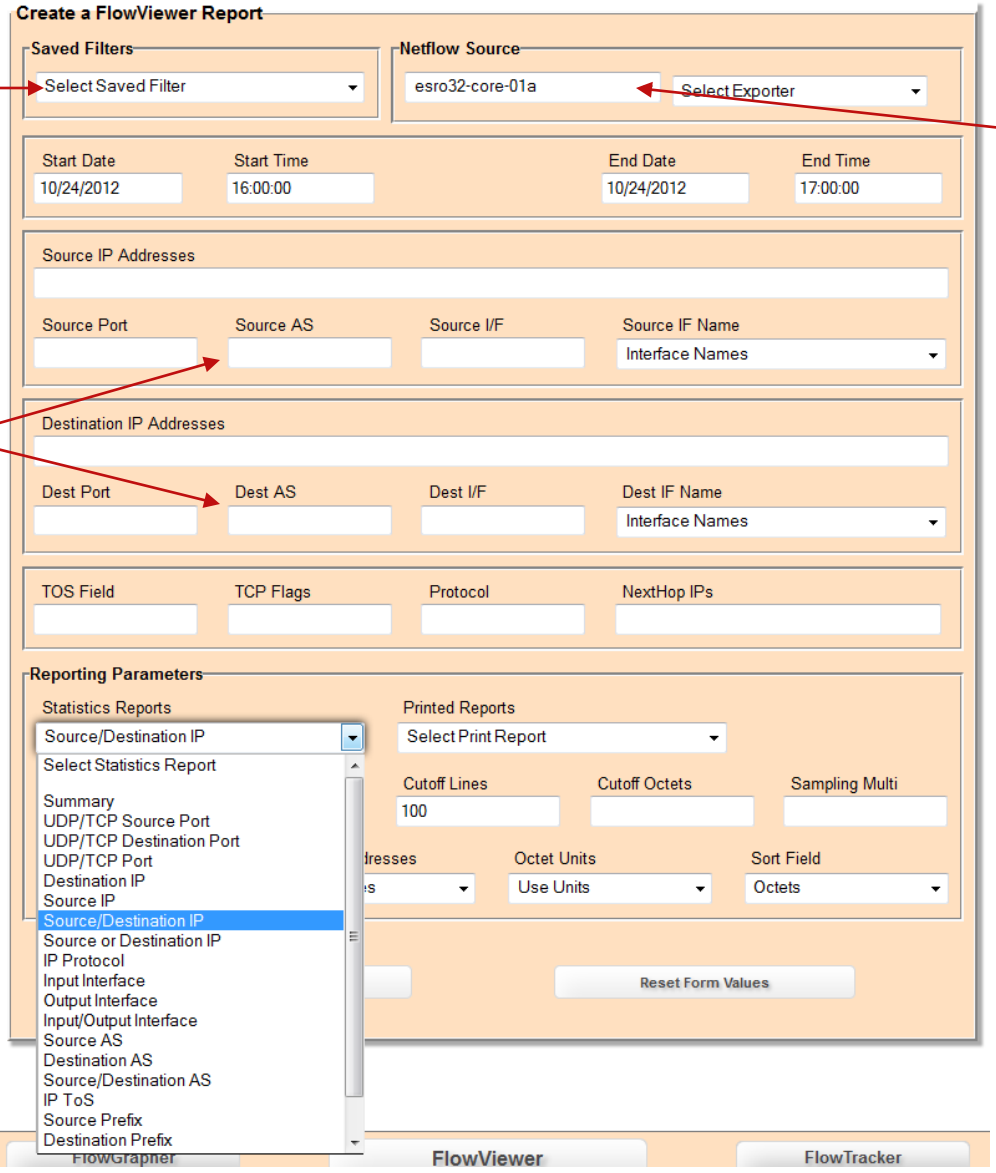
FlowViewer Main Screen



FlowViewer Input Screen

FlowViewer Input Screen - 1





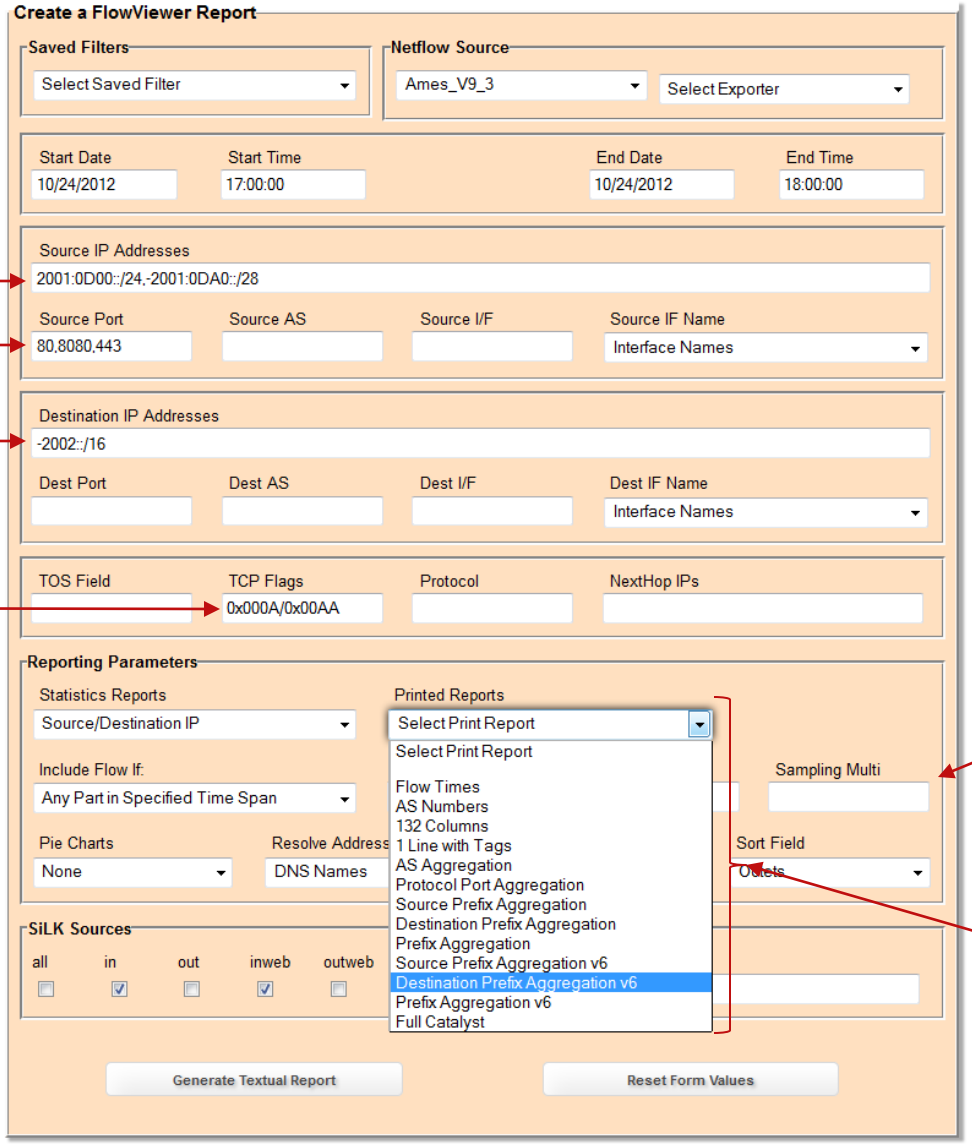
Reuse saved filter

Select from different devices

Autonomous systems (flow-tools only)

Report types

FlowViewer Input Screen - 3



Excluding within a network

Multiple entries

Excluding
(works on all fields)

TCP Flags

When using SiLK devices

Sampling multiplier

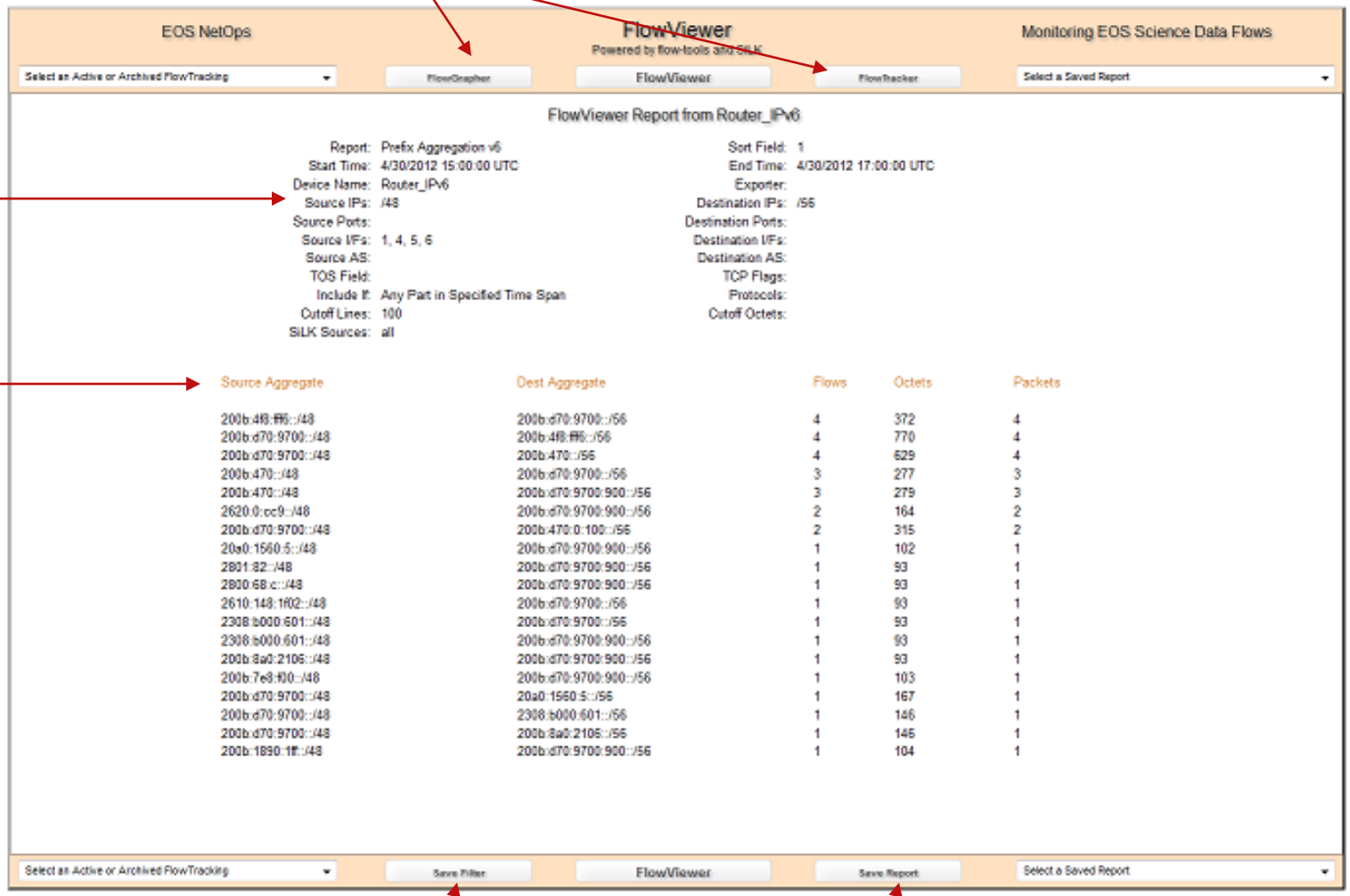
Additional reports

FlowViewer Report

Can switch to other tools with filtering criteria preserved

Aggregation filtering

Sortable by column



Save the filter

Save the report

Setting up a FlowGrapher Report

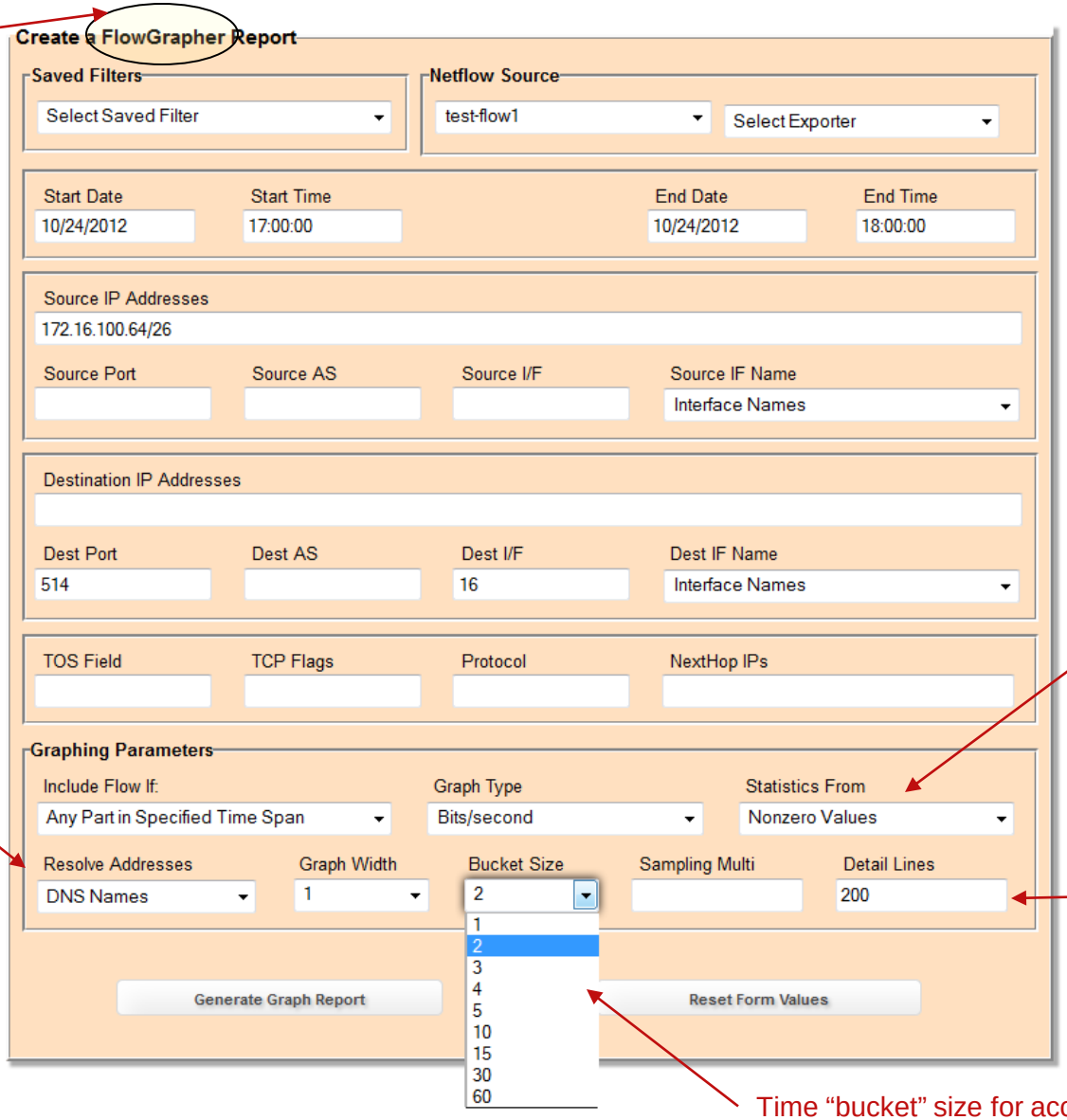
Same filtering criteria

Resolved host names or IP addresses

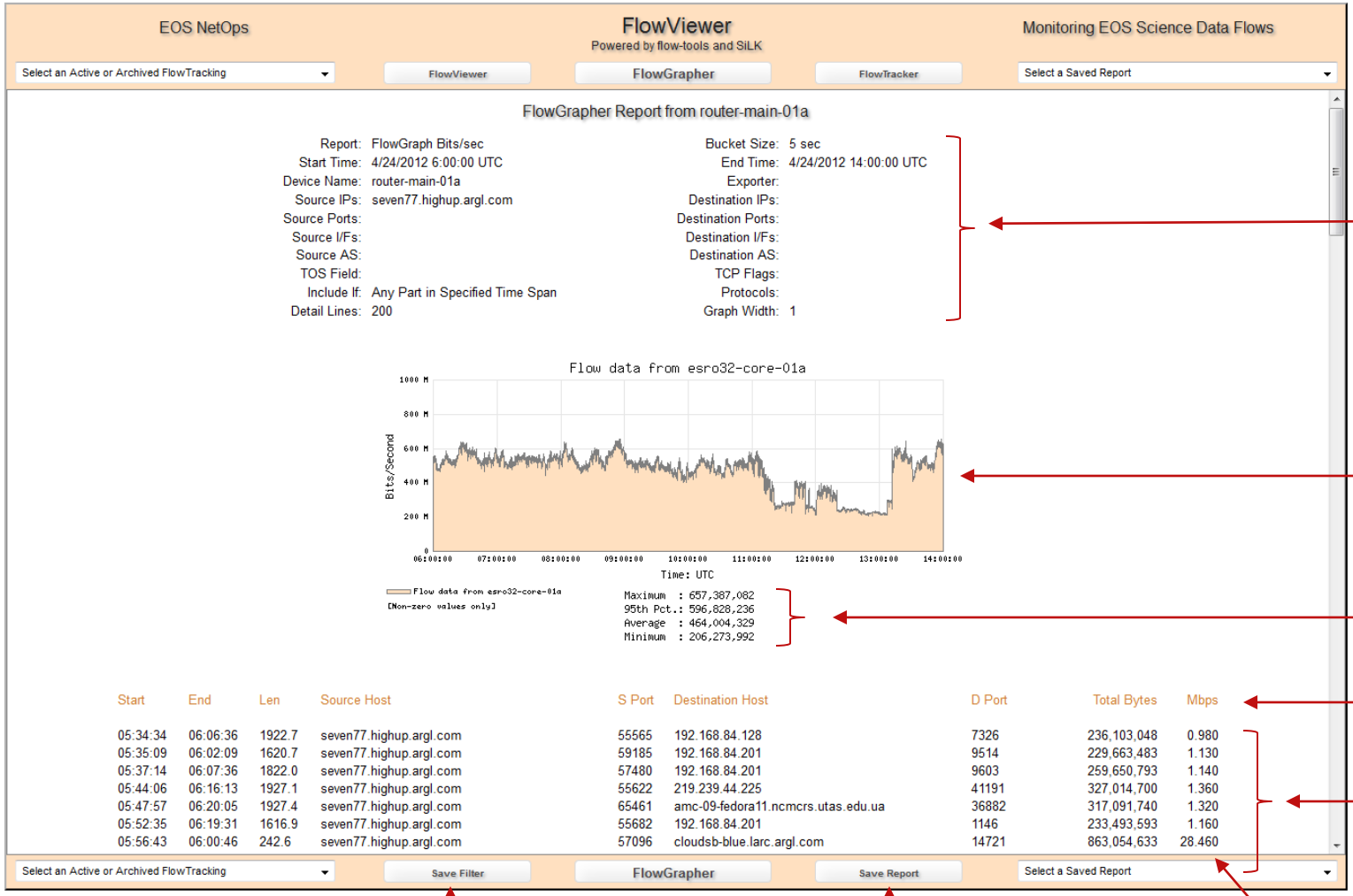
How to determine statistics (Max, 95th, Avg, Min)

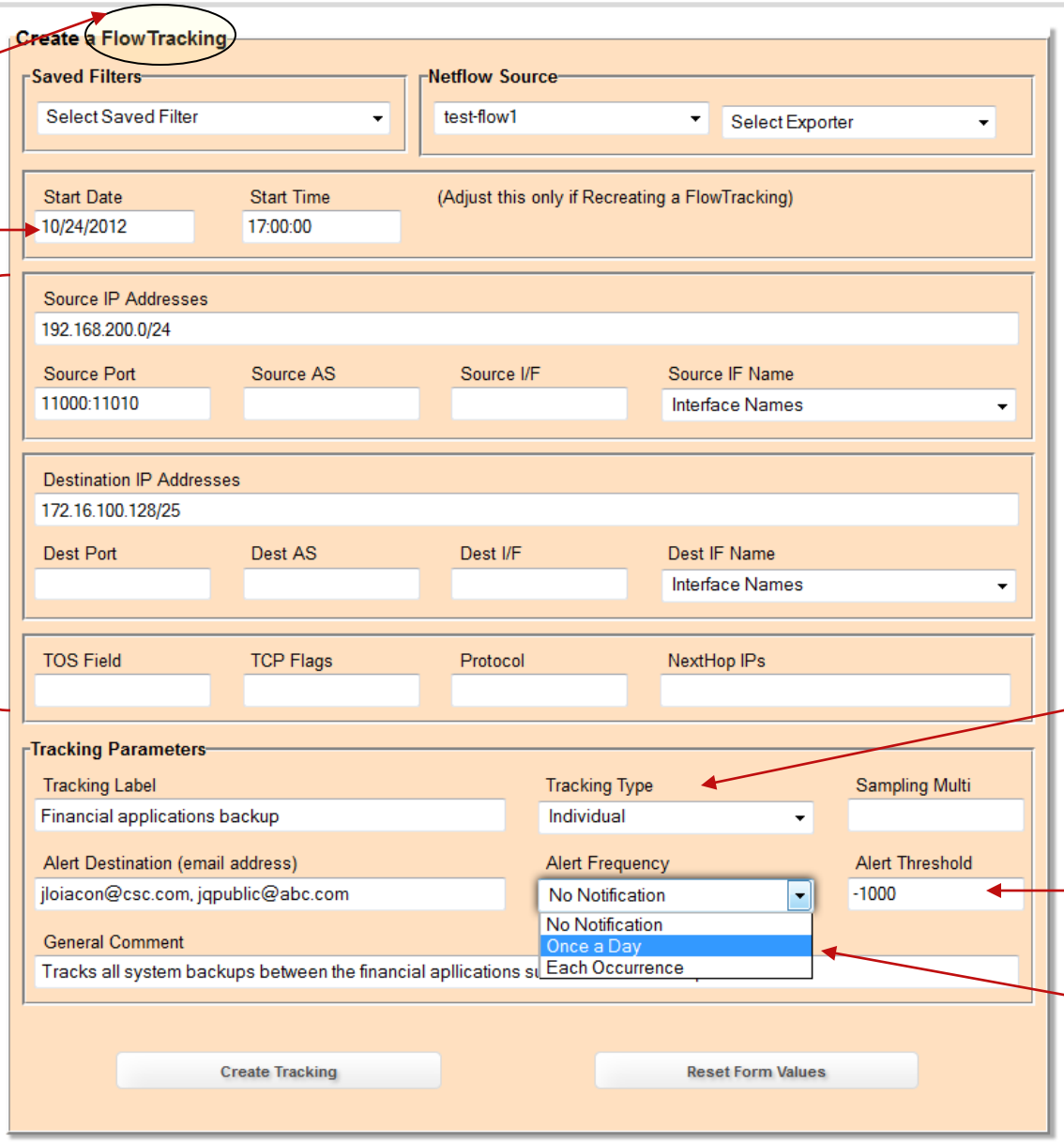
Number of longest flows to list in detail

Time "bucket" size for accumulating bits / period



FlowGrapher Report





Creating a FlowTracking

Option to start a FlowTracking in the past

Same filtering criteria

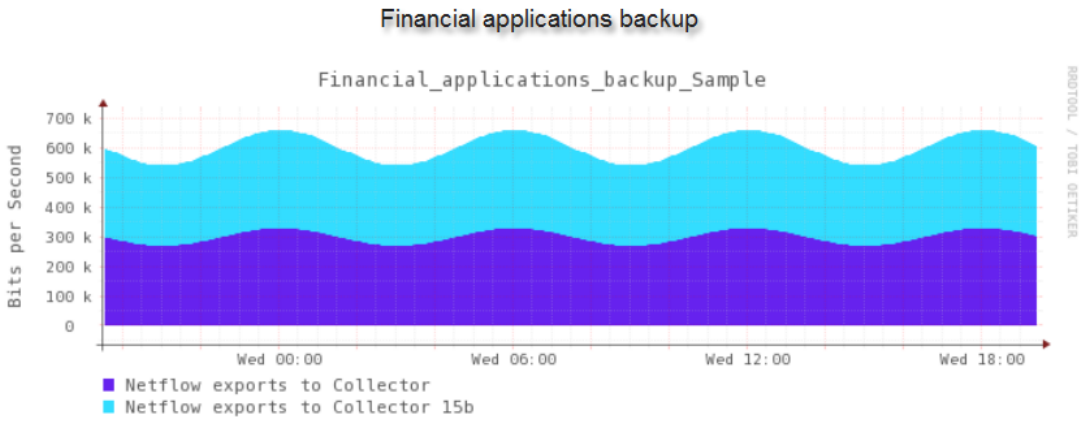
Individual or Group FlowTrackings

Email alerting

Alert thresholds

Alert frequency choices

'Groups' stack Individual FlowTrackings →



Select Individual FlowTracking Group components →

Select an existing Tracking to be a component of this Group:

Select a Component: ASTER to GSFC After

Place this Component: Above the X-axis

Select a Color: Auto Mixed

Add Component | Reset Values

← Can have components above and below X-axis

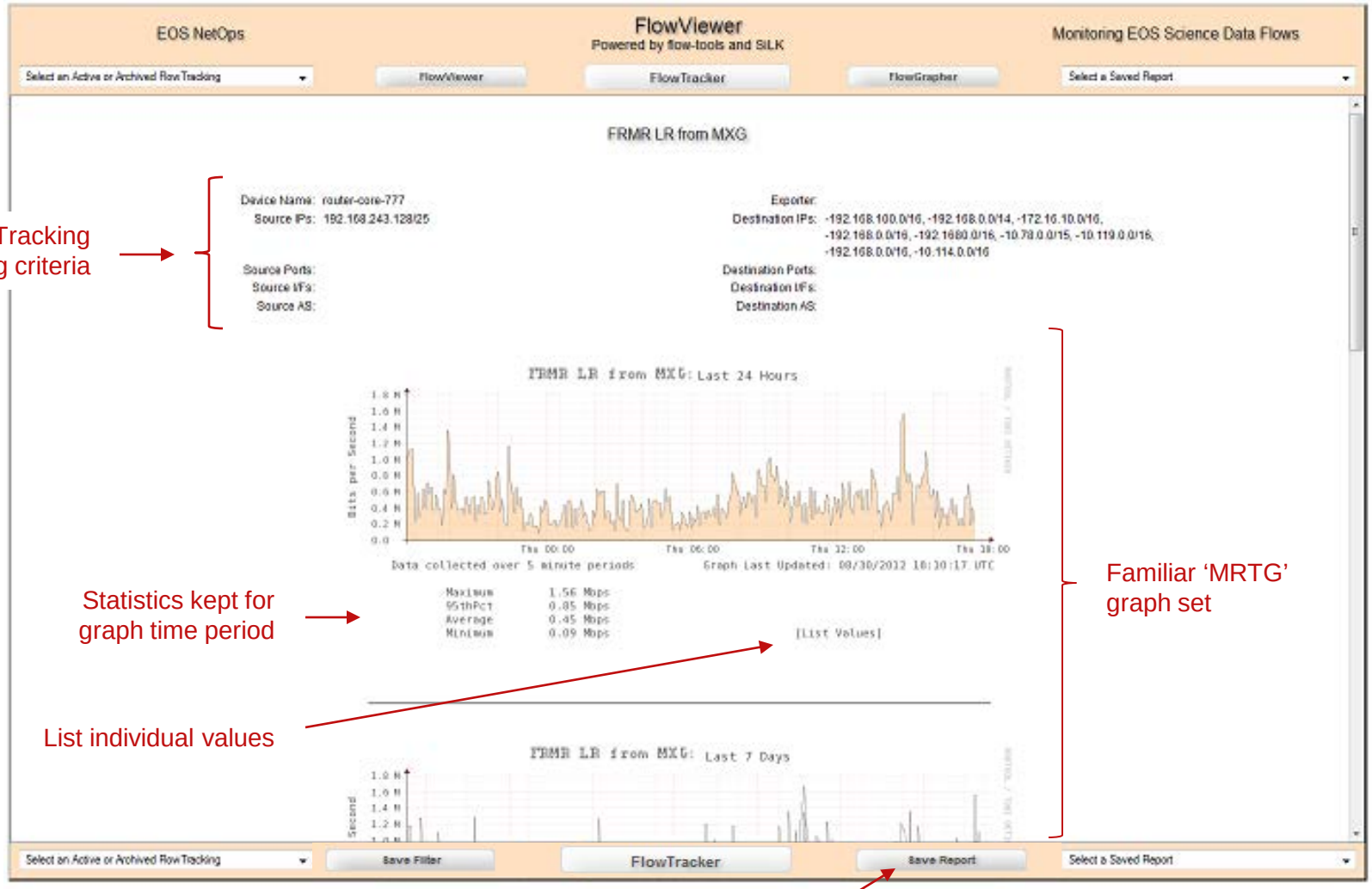
This group is composed of these components:

Adjust Group components →

Netflow exports to Collector 15b	Above 02	auto mixed2	New Color:	auto mixed2	Move:	Leave Alone
Netflow exports to Collector	Above 01	auto mixed1	New Color:	auto mixed1	Move:	Leave Alone

Adjust the Group | Reset Values

FlowTracker Report – General Example



FlowTracking filtering criteria

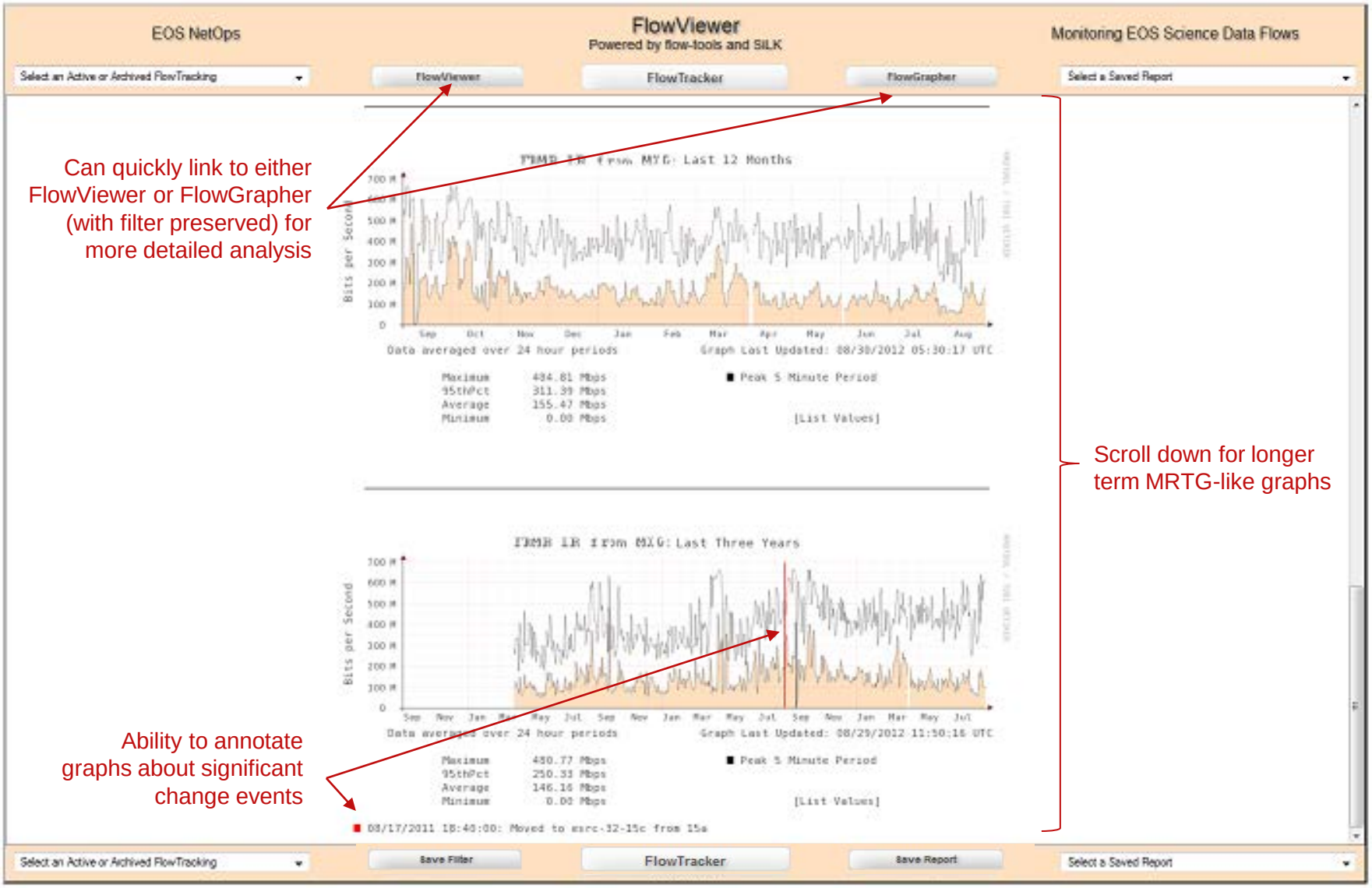
Statistics kept for graph time period

List individual values

Familiar 'MRTG' graph set

Save Report

FlowTracker Report – General Example, cont.



FlowTracker Report – Group Example

This FlowTracking documents the delivery of NPP data to the University of Wisconsin. One can see a switch from two (Atmospheric Science) servers to one only, and then all to the other of the pair.

Access to all saved reports

This is an example where you might want to save a FlowTracking

FlowTracker Report – Group Case Study

Each legend item 'hyperlinks' back to the Individual FlowTracking

This example depicts a situation where traffic shaping was invoked to manage limited network resources. This FlowTracking Group helps identify if perhaps there is one 'big player' for which a different network arrangement might mitigate the problem

Pulldown of all FlowTrackings

Listing of all FlowTrackings

Ability to ‘Revise’, ‘Rename’, ‘Archive’, ‘Remove’, and ‘Restore’ FlowTrackings

Case Studies

Components of an Interface

Satellite data in

Science data out

To service provider

Gray line preserves highest 5-minute measurement over the longer term graphs

These graphs help NASA monitor an expensive high-rate circuit between a polar ground station in Norway and the GSFC in Maryland. The circuit is shared with other Federal agencies through the use of MPLS tunnels.

This depression of peak values indicates that there may be an issue with the network or the MPLS tunnel (or the servers, or software or, …)

EOSDIS NASA's Earth Observing System Data and Information System

EOS NetOps

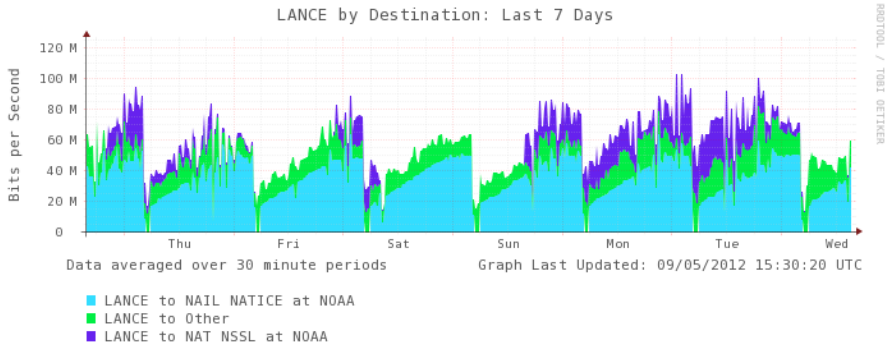
FlowViewer
Powered by flow-tools and SiLK

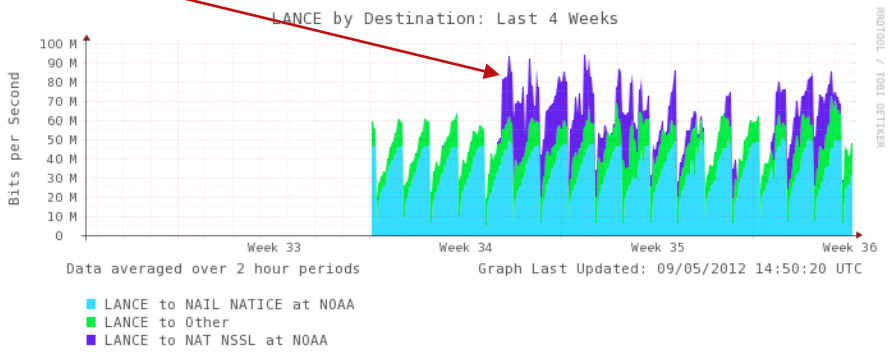
Monitoring EOS Science Data Flows

Select an Active or Archived FlowTracking | FlowViewer | FlowTracker | FlowGrapher | Select a Saved Report

Around the time of last summer's hurricane Isaac, Land, Atmosphere Near-Real-Time Capability for EOS (LANCE-MODIS*) system managers noted a sharp increase in traffic.

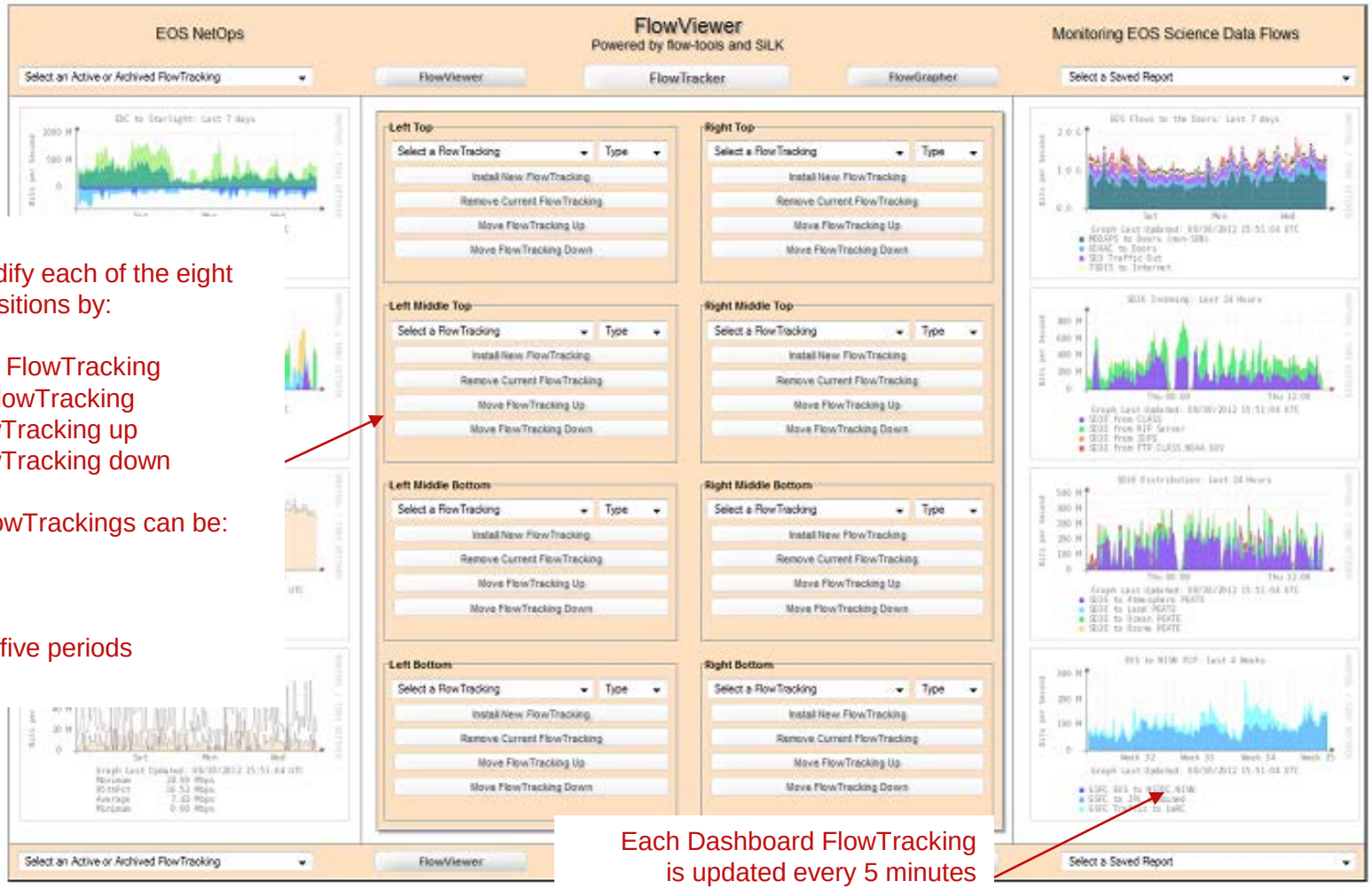
The FlowTracker Re-create capability was invoked to create a FlowTracking Group which isolated the new user that had come on line: the National Severe Storms Laboratory.





* MODIS - Moderate Resolution Imaging Spectroradiometer

Select an Active or Archived FlowTracking | FlowViewer | FlowTracker | FlowGrapher | Select a Saved Report



Users can modify each of the eight Dashboard positions by:

1) Install new FlowTracking
2) Remove FlowTracking
3) Move FlowTracking up
4) Move FlowTracking down

Dashboard FlowTrackings can be:

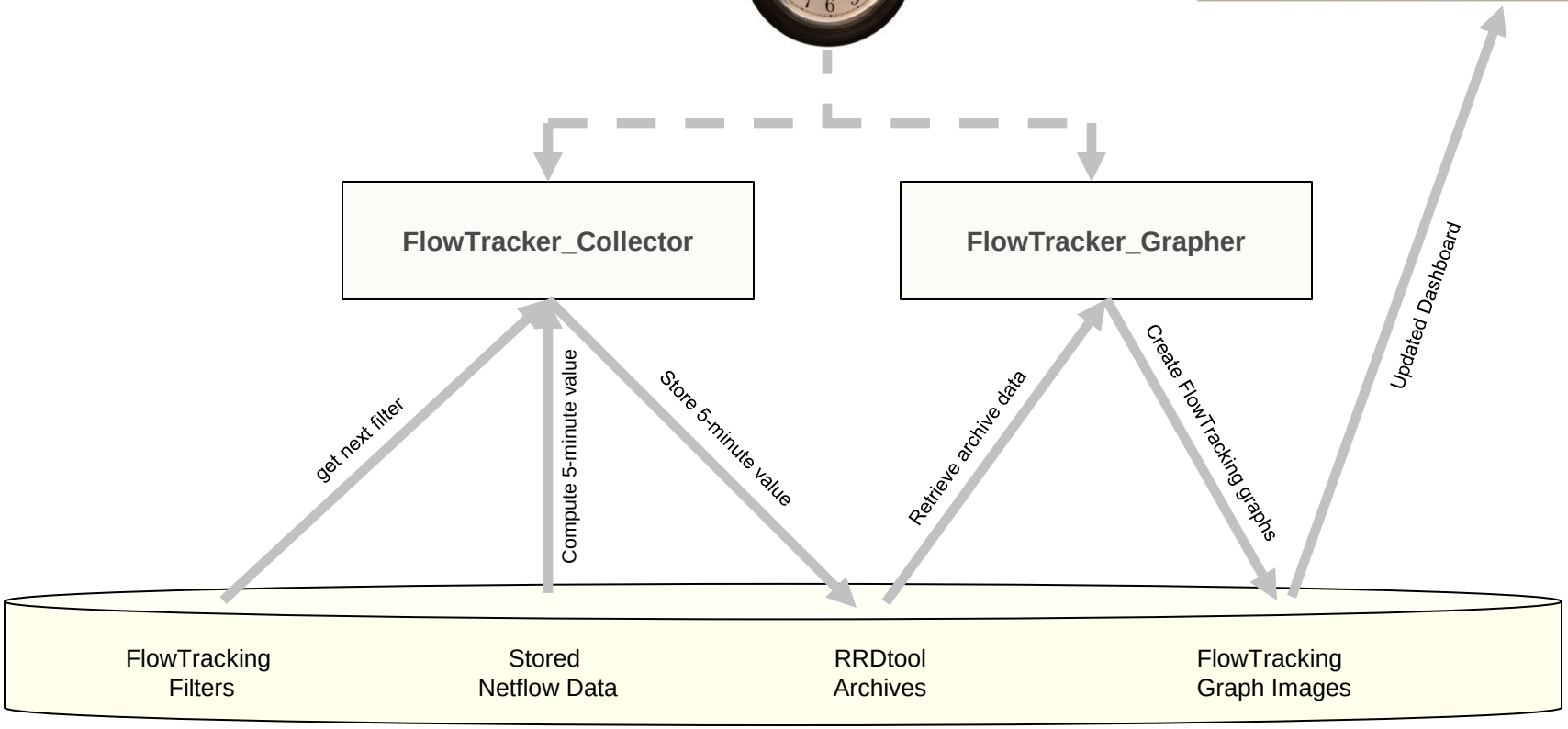
1) Individual
2) Group
3) Any of the five periods

.

Each Dashboard FlowTracking is updated every 5 minutes

Each Dashboard graph links back to the original FlowTracking

Upon FlowViewer installation, the FlowTracker_Collector and FlowTracker_Grapher scripts are placed in the Linux background. They will “wake up” every five minutes and collect a 5-minute value for each active FlowTracking. The FlowTracking and Dashboard graphs are updated with the latest data point.



- FlowViewer distribution includes “analyze_netflow_packets” utility
- FlowViewer has supported flow-tools for over five years; but is new to SiLK
- Integration with SiLK may not be optimized as a result
- Would welcome SiLK related improvement suggestions
- At the same time … some ‘requests’ of SiLK ☺. Please include:
  - IPFIX Information Element (IE) [5]: ipClassOfService
  - IPFIX Information Element (IE) [16]: bgpSourceAsNumber
  - IPFIX Information Element (IE) [17]: bgpDestinationAsNumber
  - IPFIX Information Element (IE) [70]: mplsLabelStackSection
  - IPFIX Information Element (IE) [71]: mplsLabelStackSection2
  - IPFIX Information Element (IE) [72]: mplsLabelStackSection3

Thank You

Joe Loiacono
Network Engineer, CSC
jloiacon@csc.com

http://earthdata.nasa.gov/esdis

NASA Official: Kevin Kranacs
Manager, ESDIS Networks

FlowViewer is available from:
https://sourceforge.net/projects/flowviewer